Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

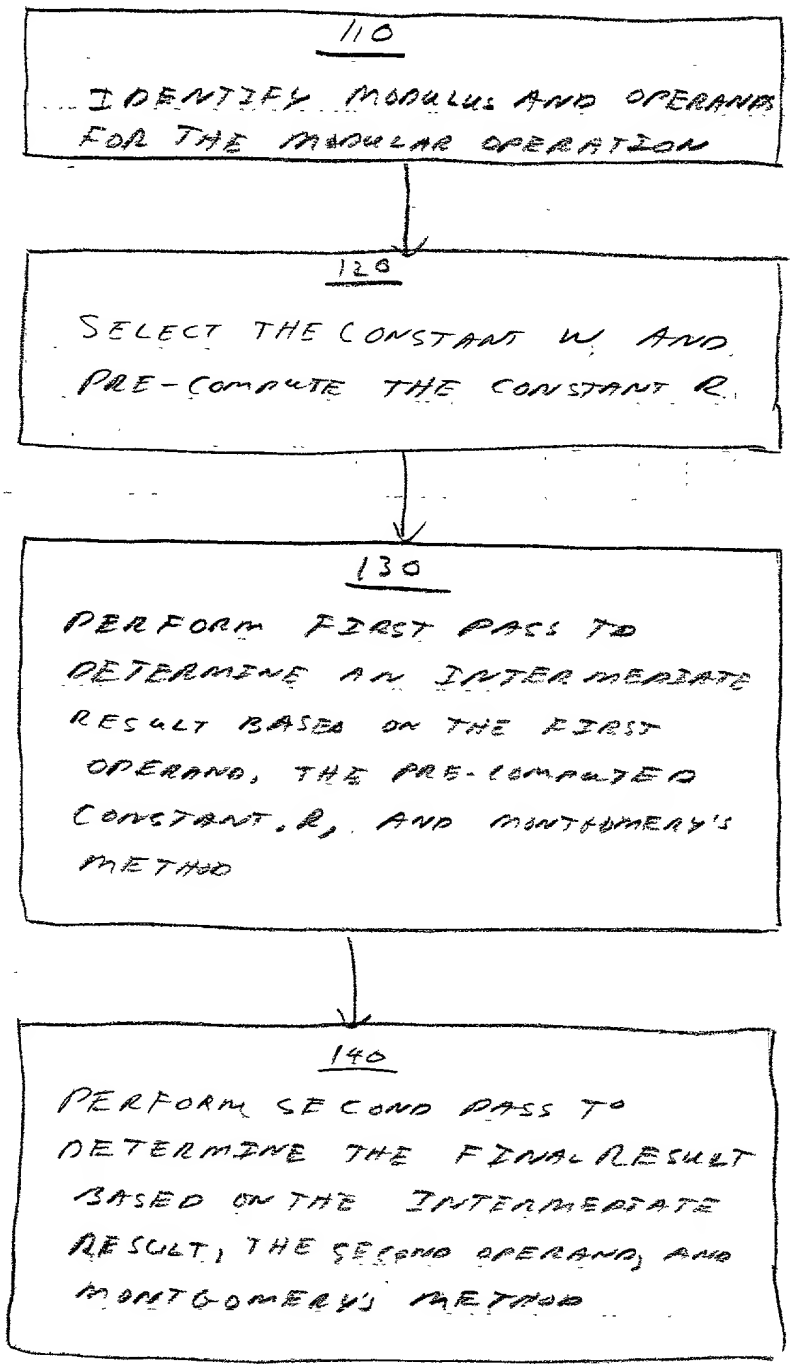


FIG 1

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

2/25

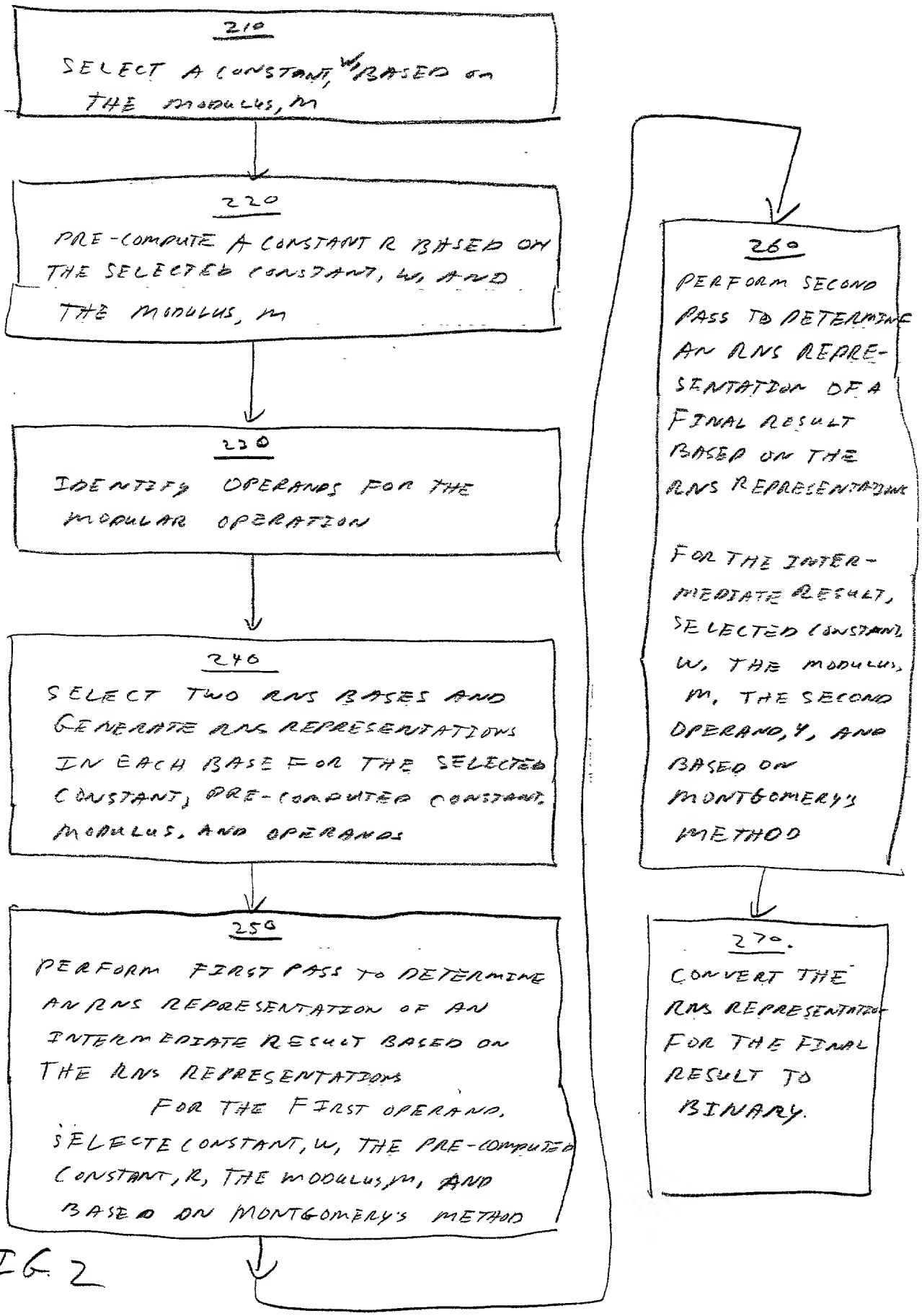


FIG 2

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

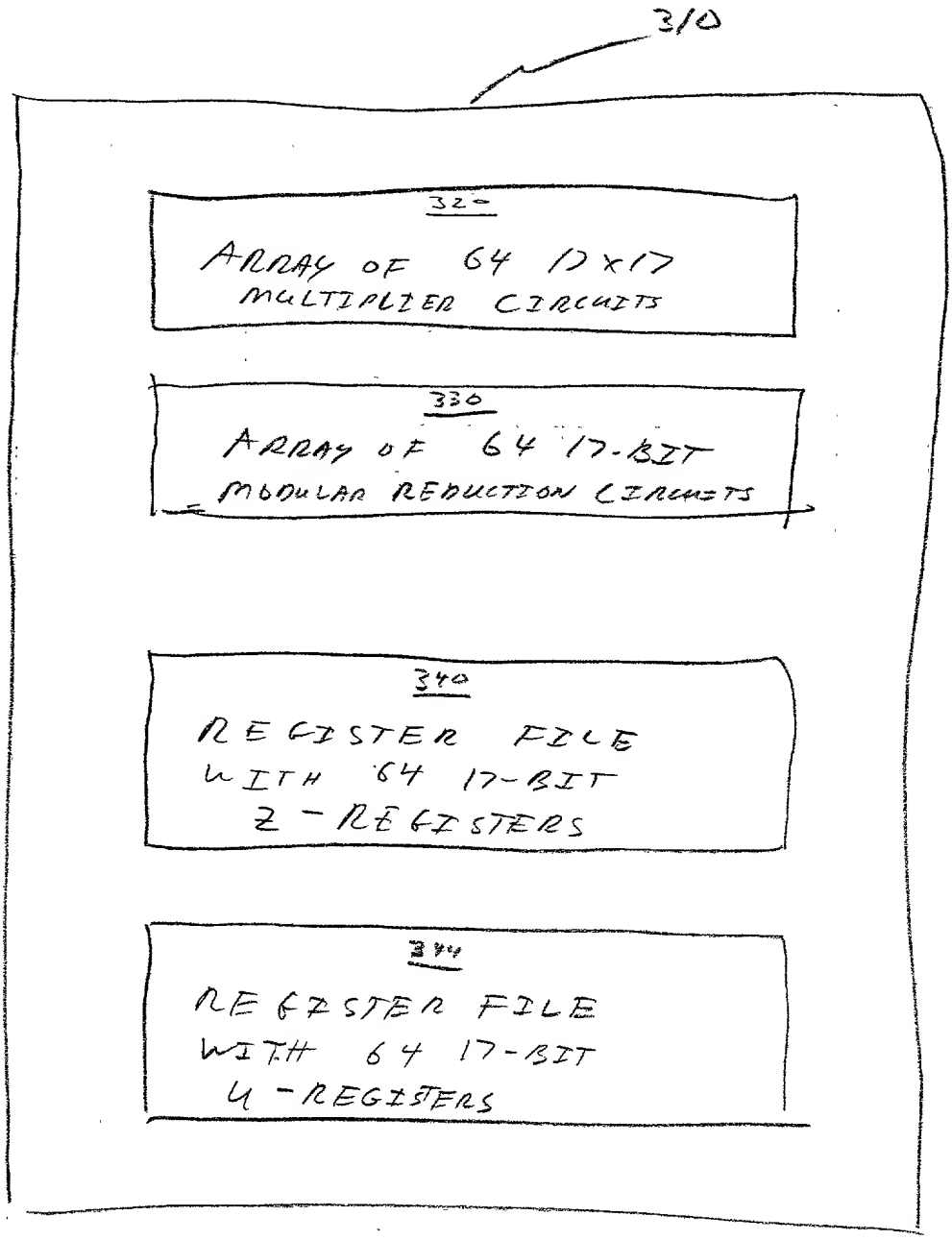


FIG. 3A

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

4/25

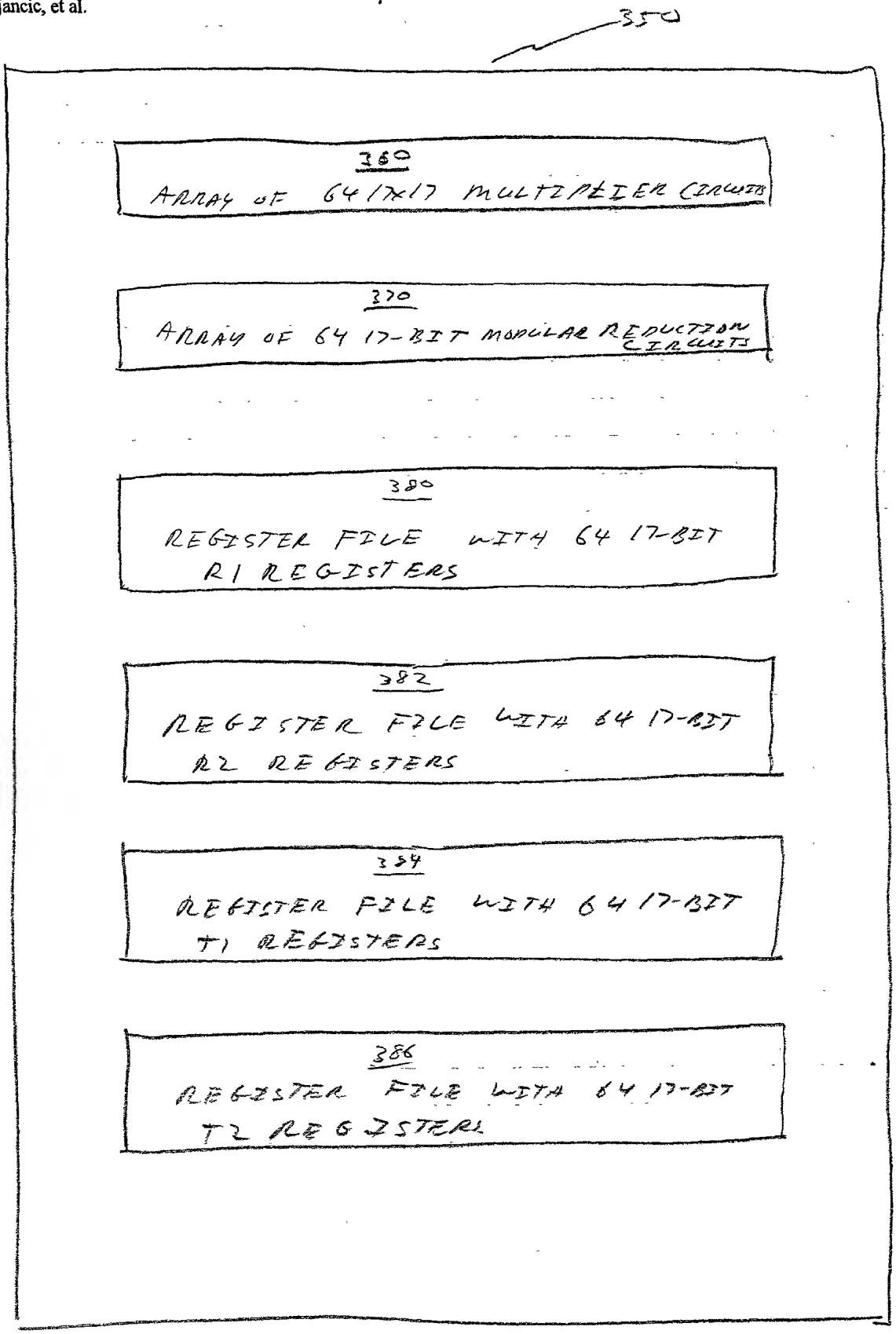


FIG 3B

5/25

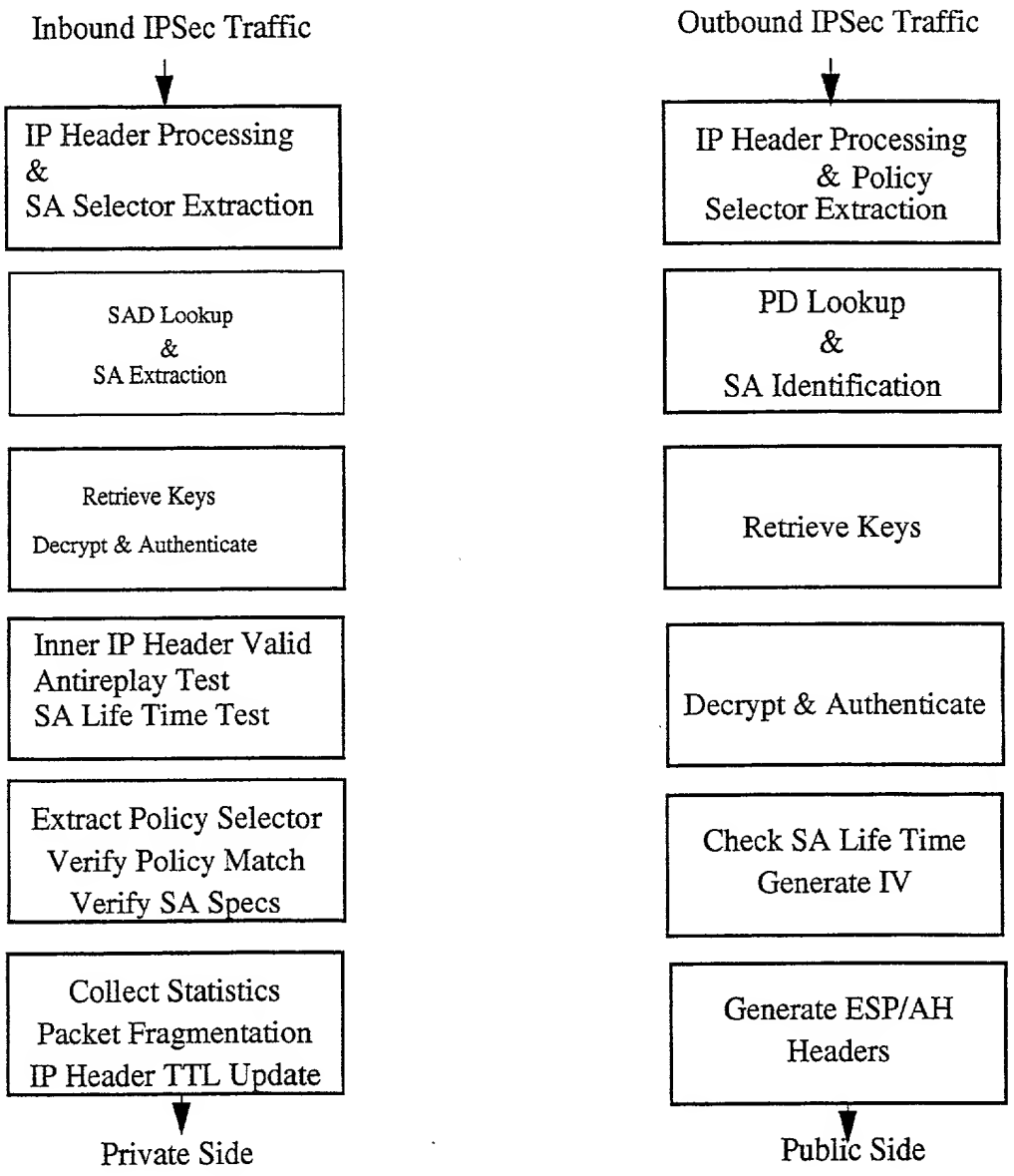

Inbound IPSec Traffic
IP Header Processing & SA Selector Extraction
SAD Lookup & SA Extraction
Retrieve Keys
Decrypt & Authenticate
Inner IP Header Valid
Antireplay Test
SA Life Time Test
Extract Policy Selector
Verify Policy Match
Verify SA Specs
Collect Statistics
Packet Fragmentation
IP Header TTL Update
Private Side
Outbound IPSec Traffic
IP Header Processing & Policy Selector Extraction
PD Lookup & SA Identification
Retrieve Keys
Decrypt & Authenticate
Check SA Life Time
Generate IV
Generate ESP/AH Headers
Public Side

FIG. 4

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

6/25

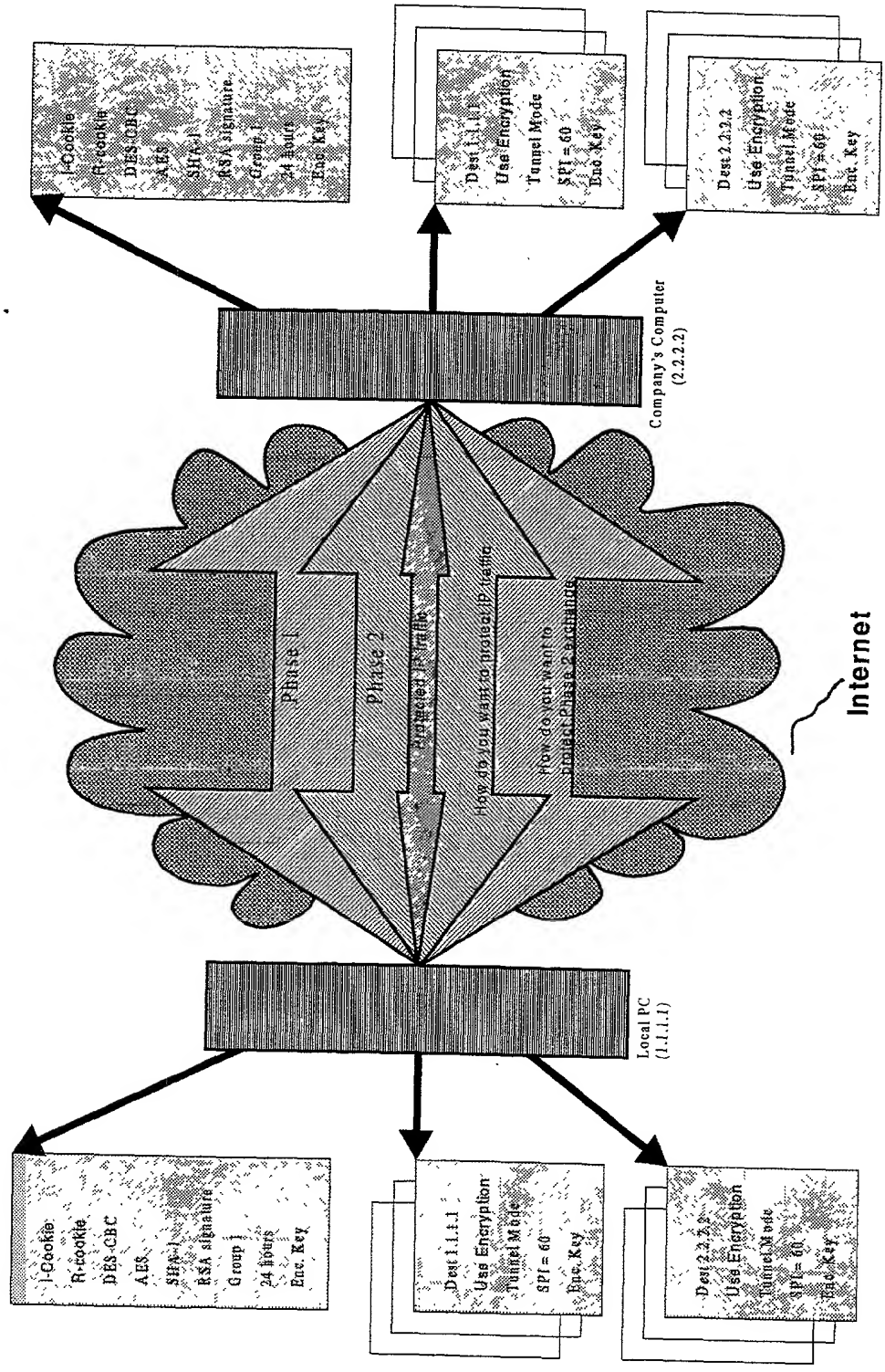


FIG. 5

7/25

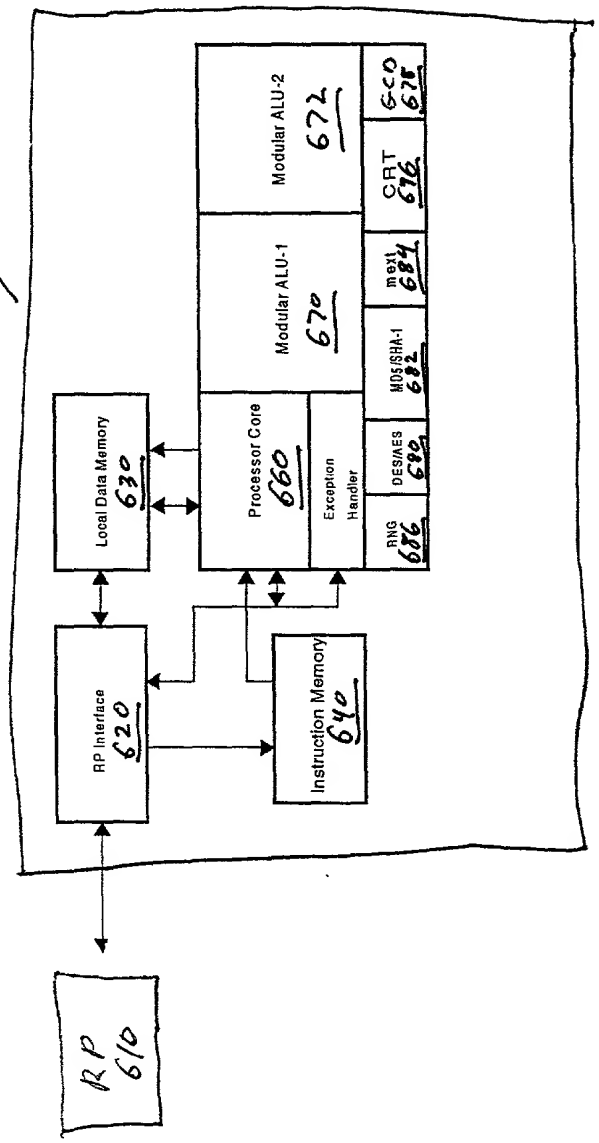
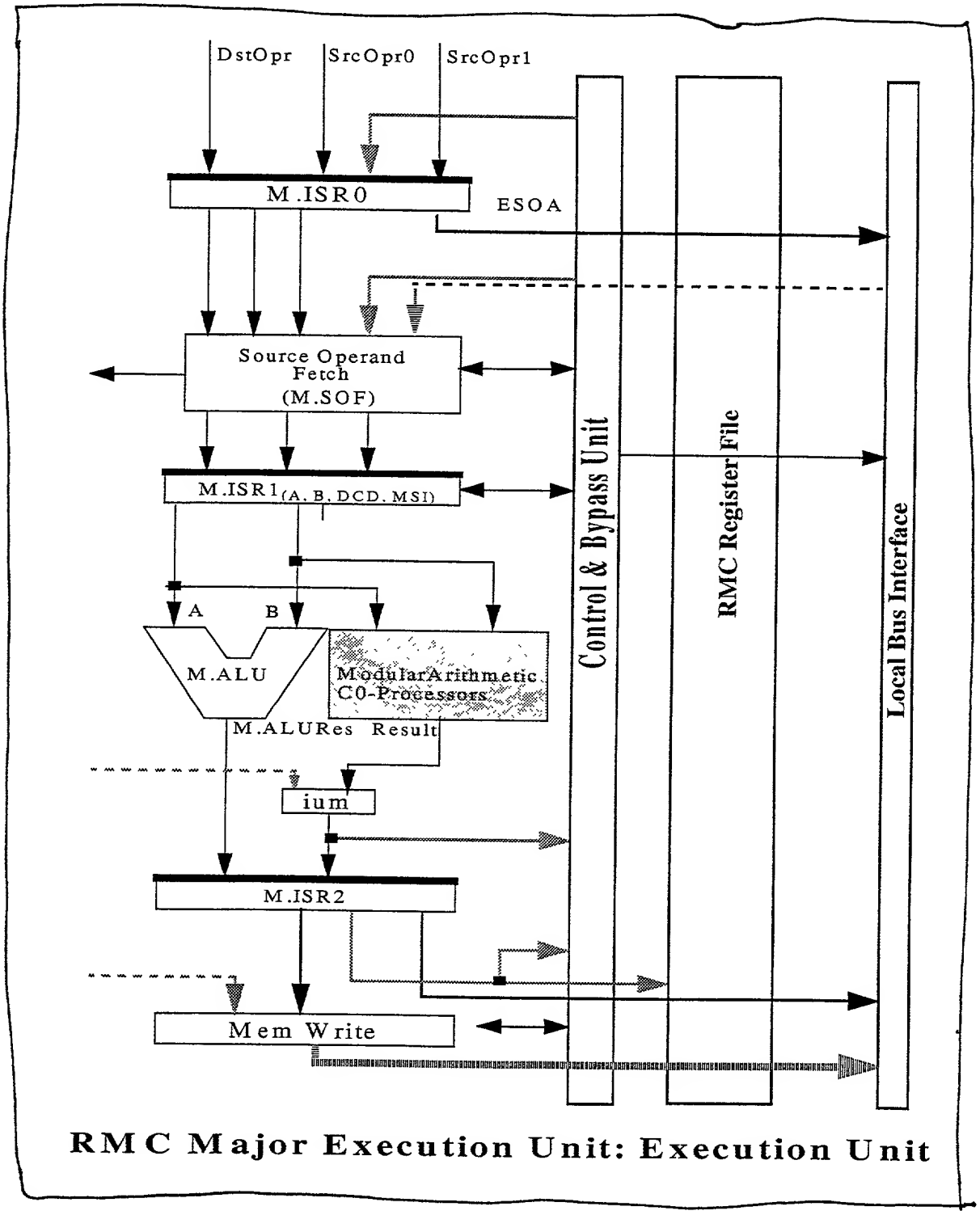


FIG. 6

8/25



RMC Major Execution Unit: Execution Unit

FIG. 7

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: Rectangular blocks on the same horizontal level overlap execution times.

⇐ - Source Overwrites Destination Register
® - Modular Multiplication with respect to w.
© - Modular Multiplication with respect to v.
∠ - RNS Conversion

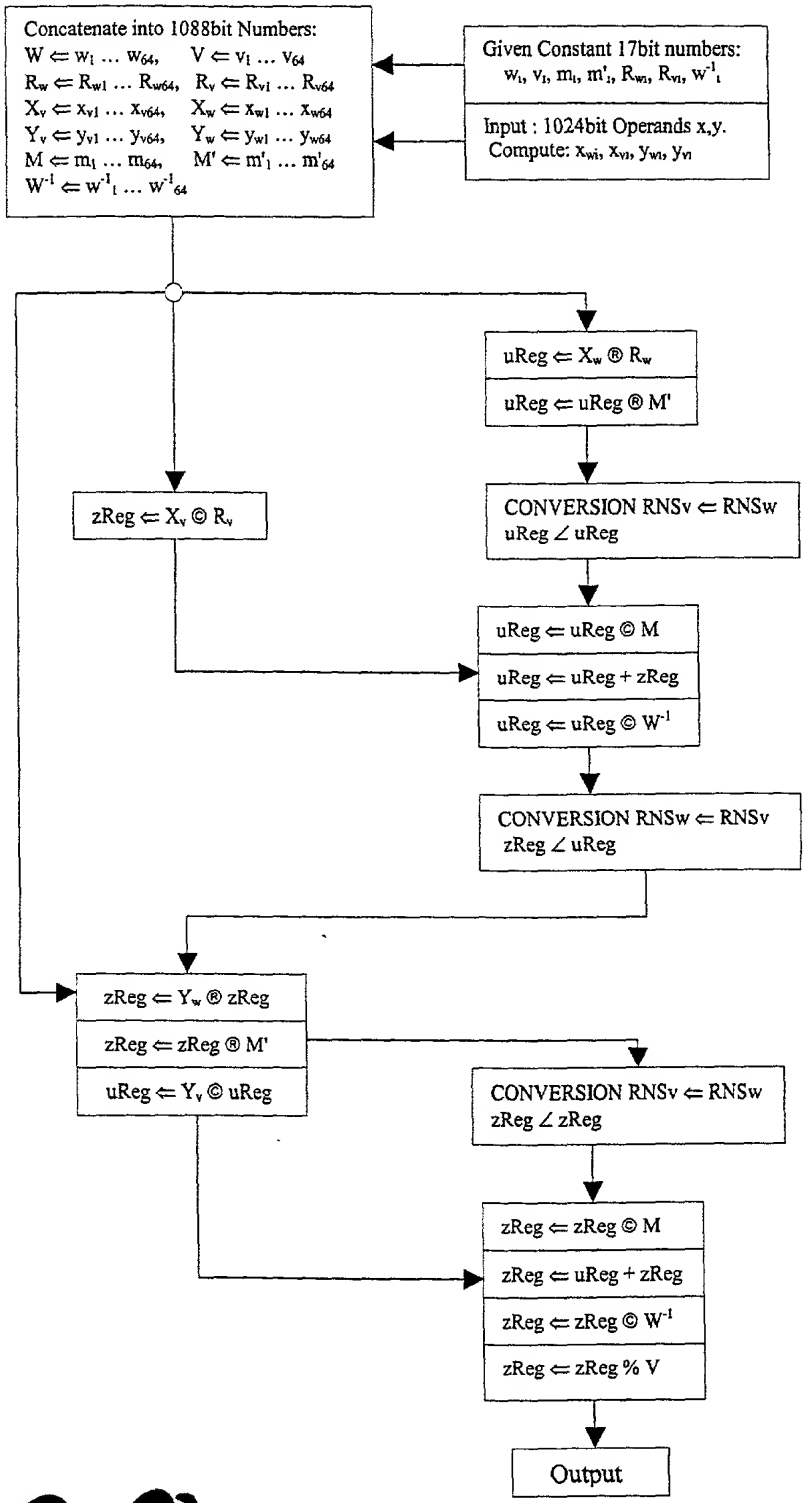


FIG. 8

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: All busses are 64x17 = 1088 bits wide.

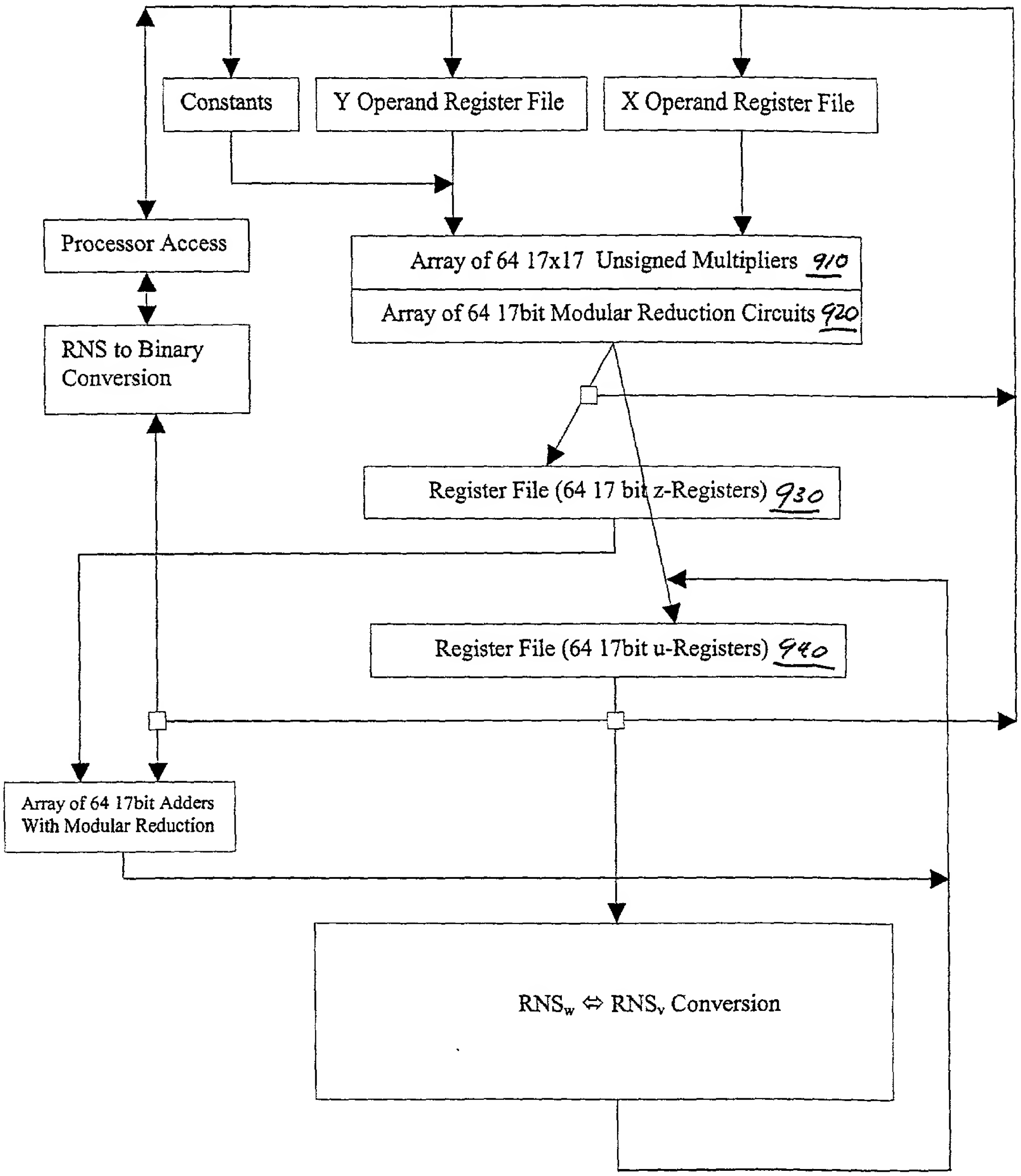


FIG.9

11/25

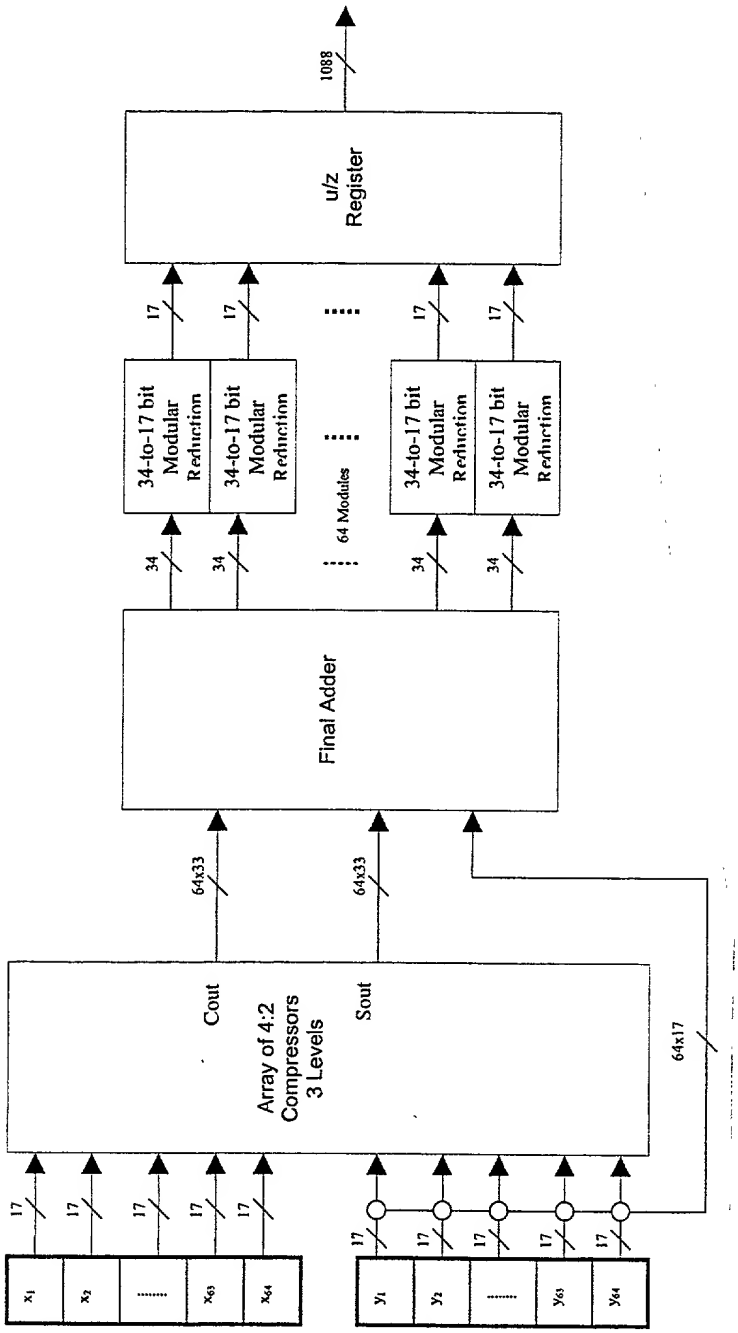


FIG. 10

12/25

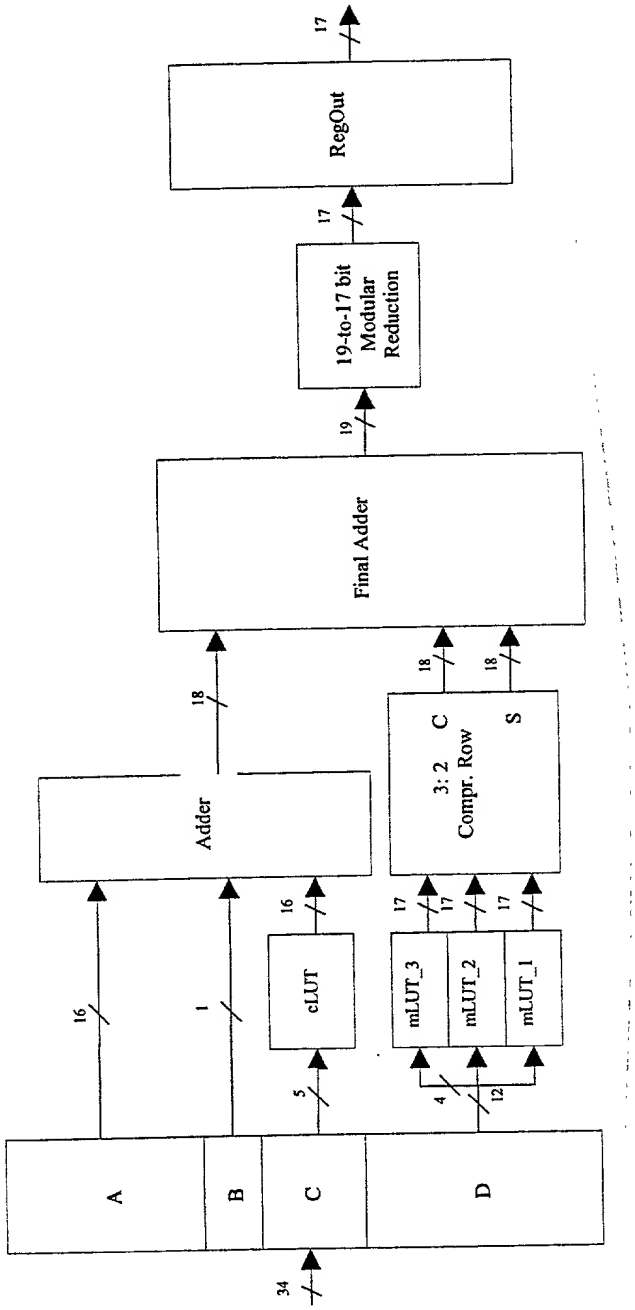

RegOut
17
19-to-17 bit Modular Reduction
19
Final Adder
18
18
Adder
3: 2 Compr. Row
C
S
16
1
cLUT
mLUT_3
mLUT_2
mLUT_1
17
17
17
16
5
4
12
A
B
C
D
34

FIG. 11

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

Note: Rectangular blocks on the same horizontal level overlap execution times.

⇐ - Source Overwrites Destination Register
® - Modular Multiplication with respect to w.
© - Modular Multiplication with respect to v.
∠ - RNS Conversion

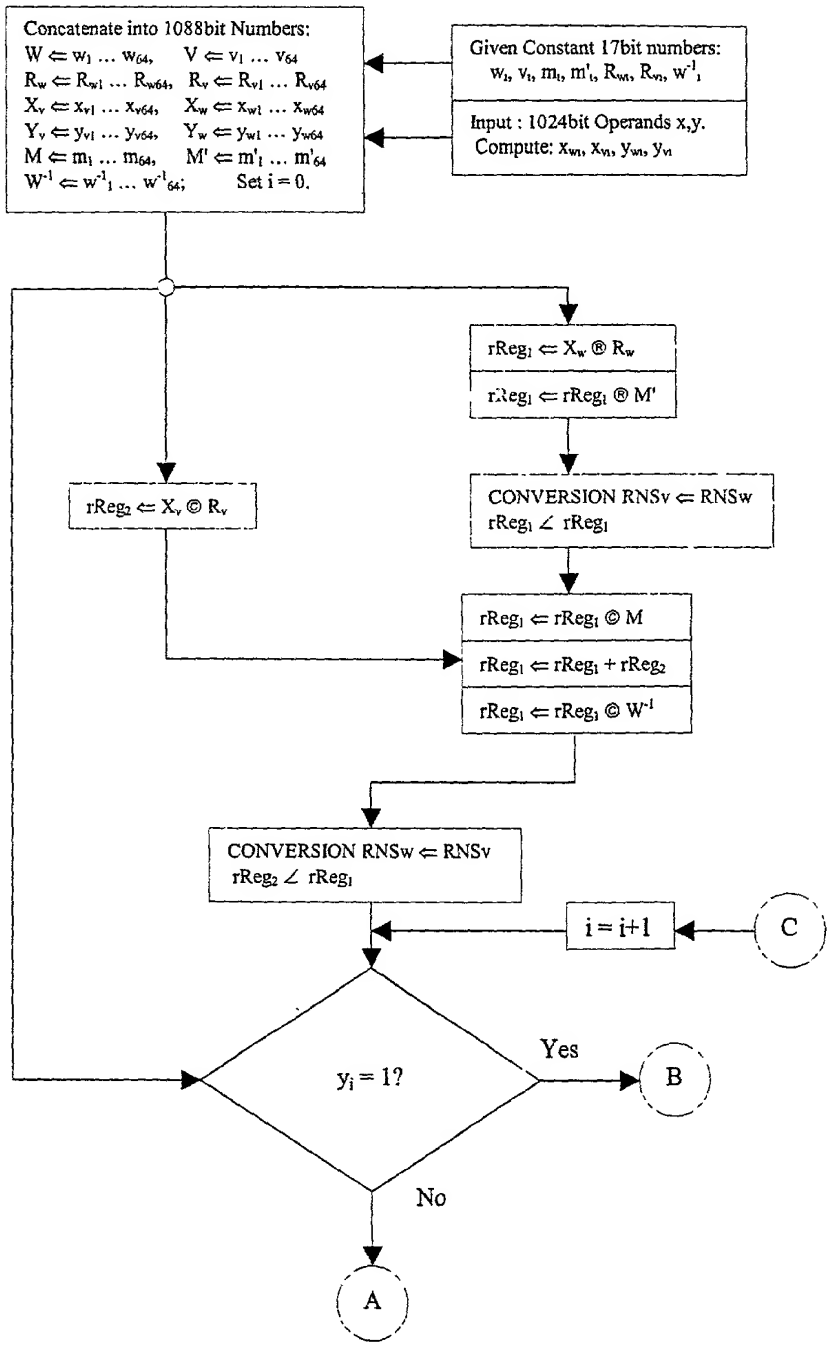


FIG. 12A

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: NYA
Docket No. 50325-0550

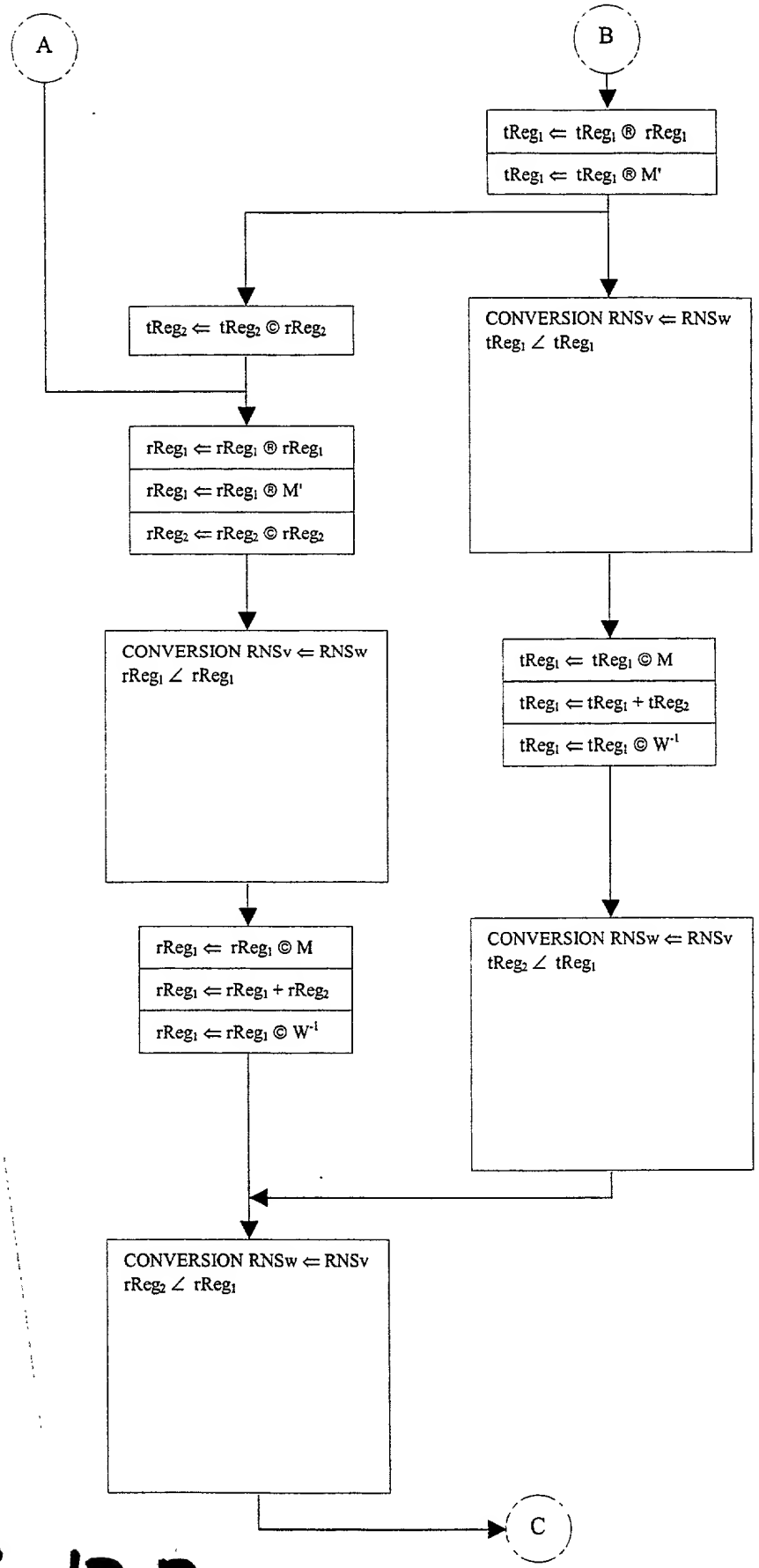


FIG. 12B

Note: All busses are 64x17 = 1088 bits wide.

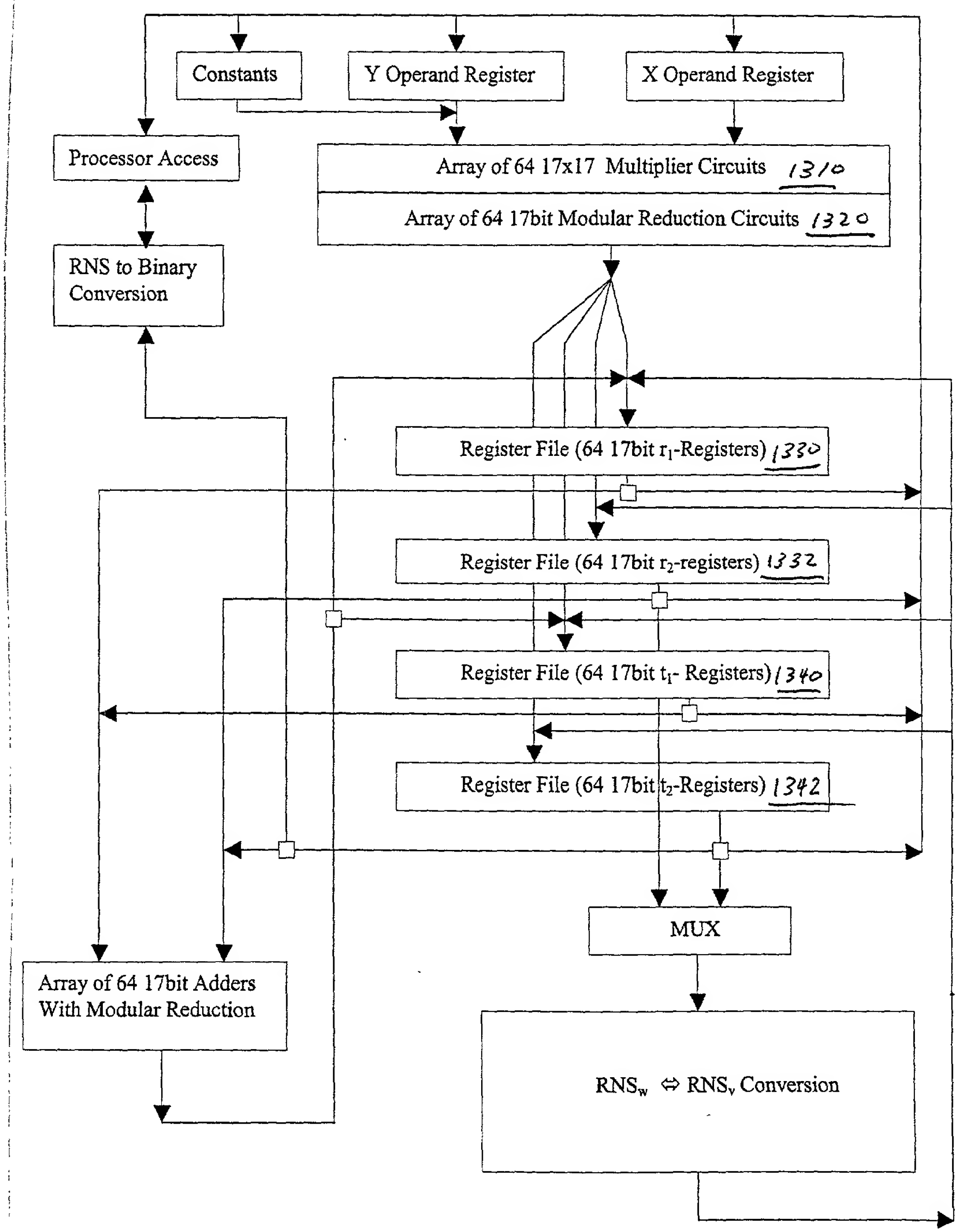


FIG. 13

16/25

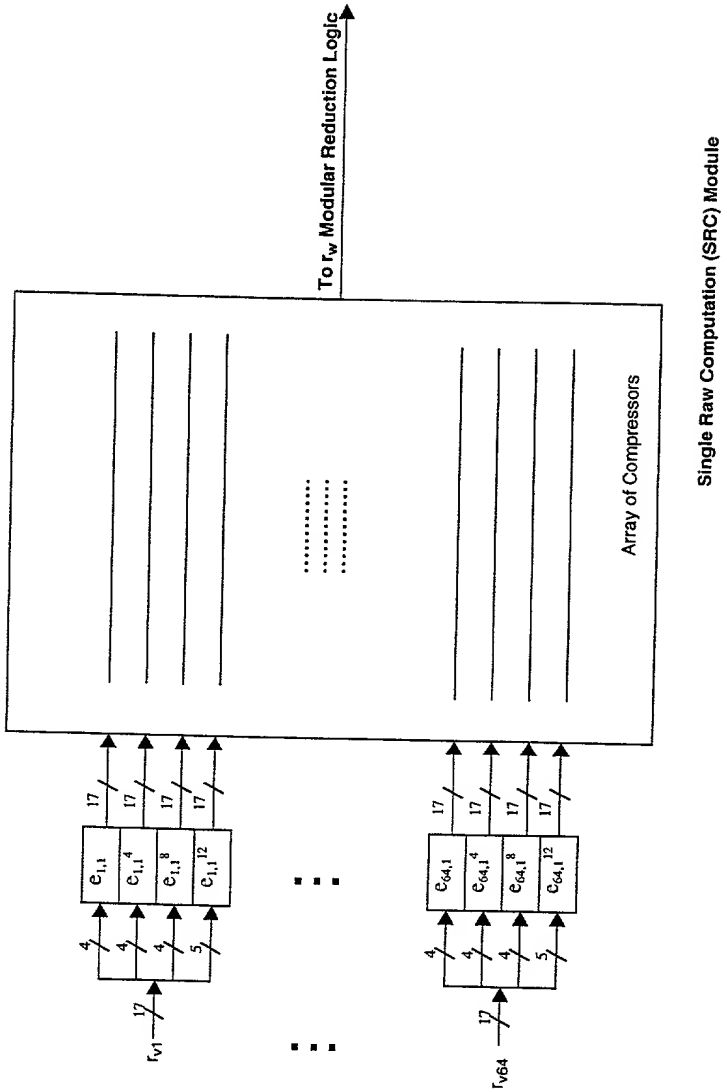

To r_w Modular Reduction Logic
Array of Compressors
Single Raw Computation (SRC) Module
17
4
5
r_{v1}
r_{v64}
$e_{1,1}$
$e_{1,1}^{4}$
$e_{1,1}^{8}$
$e_{1,1}^{12}$
$e_{64,1}$
$e_{64,1}^{4}$
$e_{64,1}^{8}$
$e_{64,1}^{12}$

FIG. 14

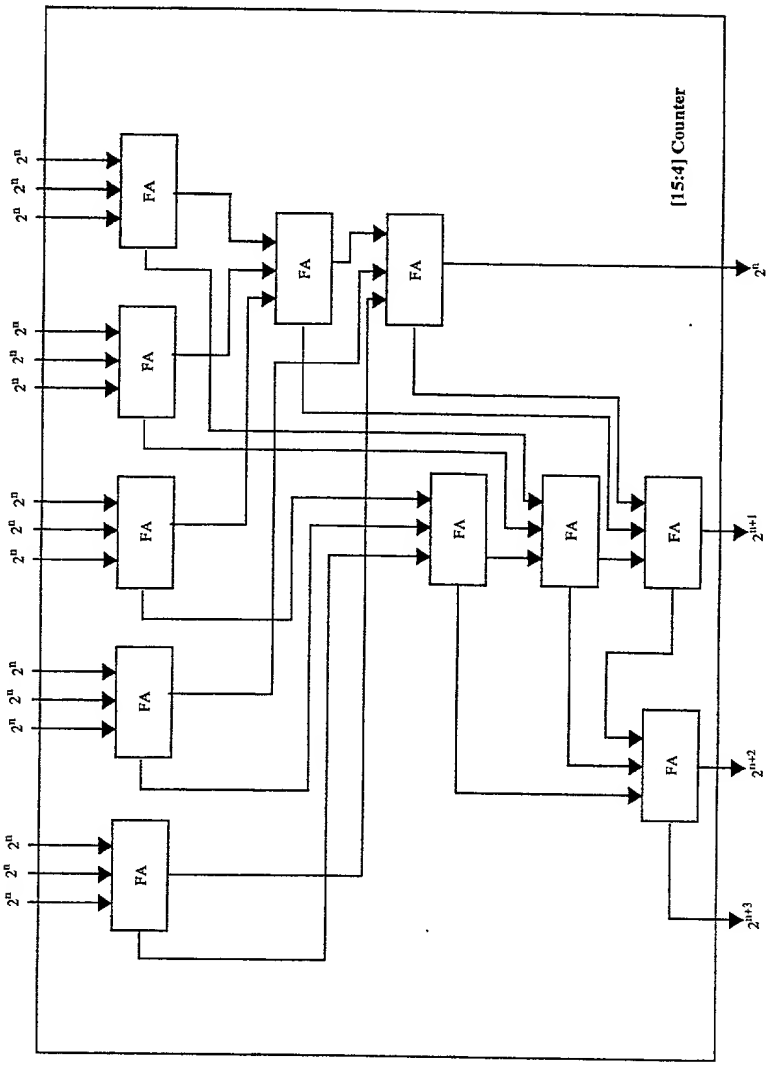


FIG. 15

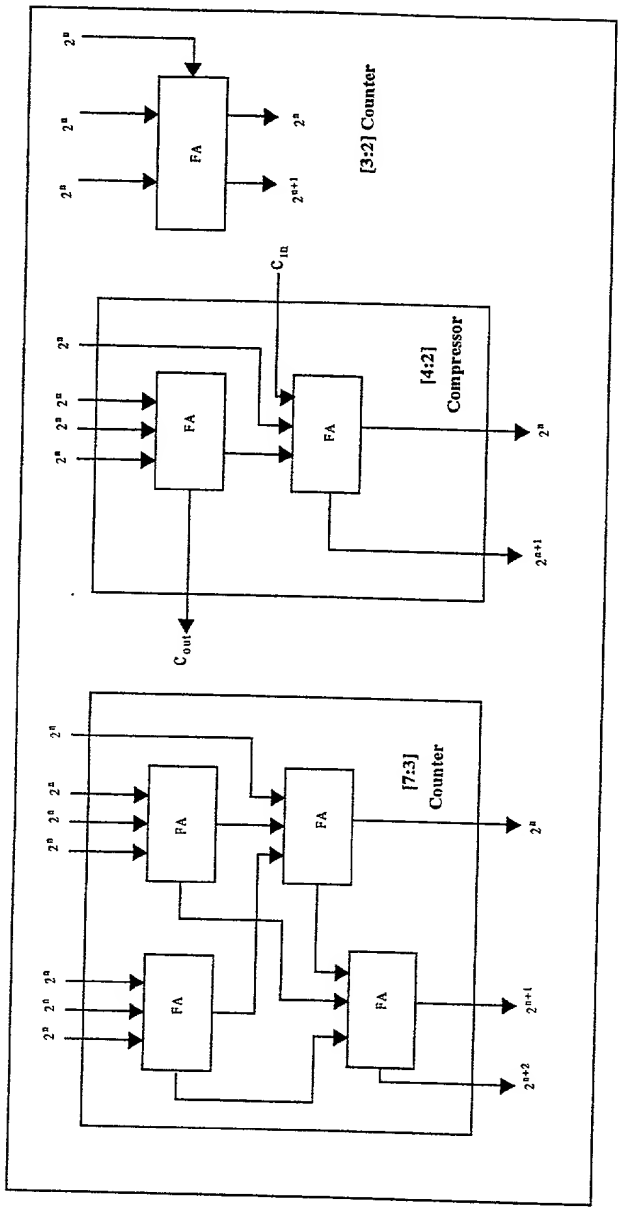

[3:2] Counter
FA
[4:2]
Compressor
FA
FA
C_{in}
C_{out}
[7:3]
Counter
FA
FA
FA
FA

FIG. 16

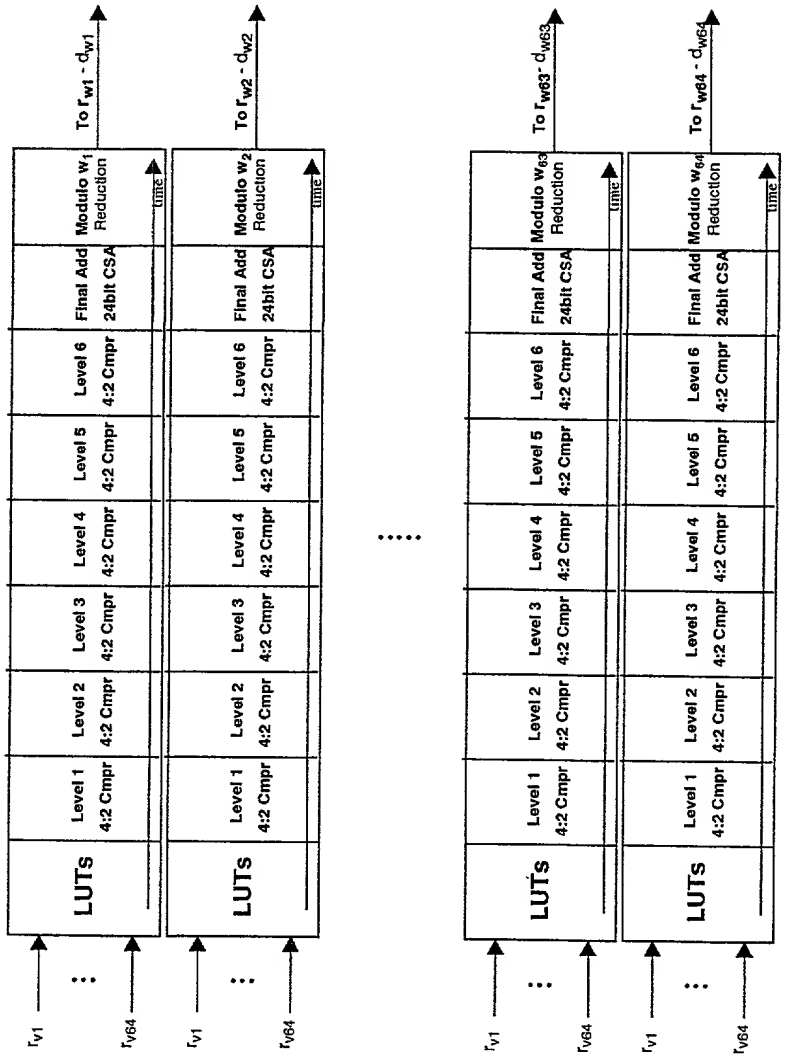

LUTs
Level 1 4:2 Cmpr
Level 2 4:2 Cmpr
Level 3 4:2 Cmpr
Level 4 4:2 Cmpr
Level 5 4:2 Cmpr
Level 6 4:2 Cmpr
Final Add 24bit CSA
Modulo w1 Reduction
Modulo w2 Reduction
Modulo w63 Reduction
Modulo w64 Reduction
time
To rw1 - dw1
To rw2 - dw2
To rw63 - dw63
To rw64 - dw64
rv1
rv64

FIG. 17

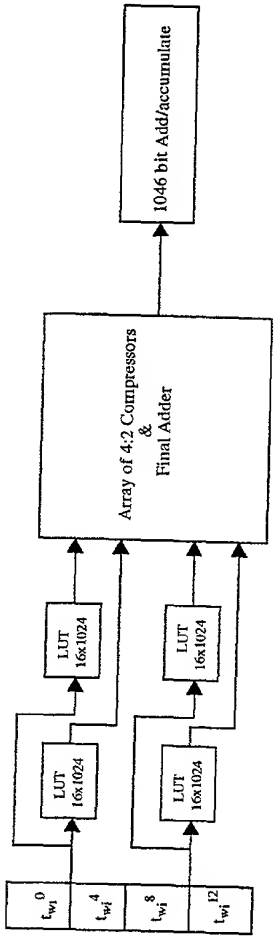


FIG. 18

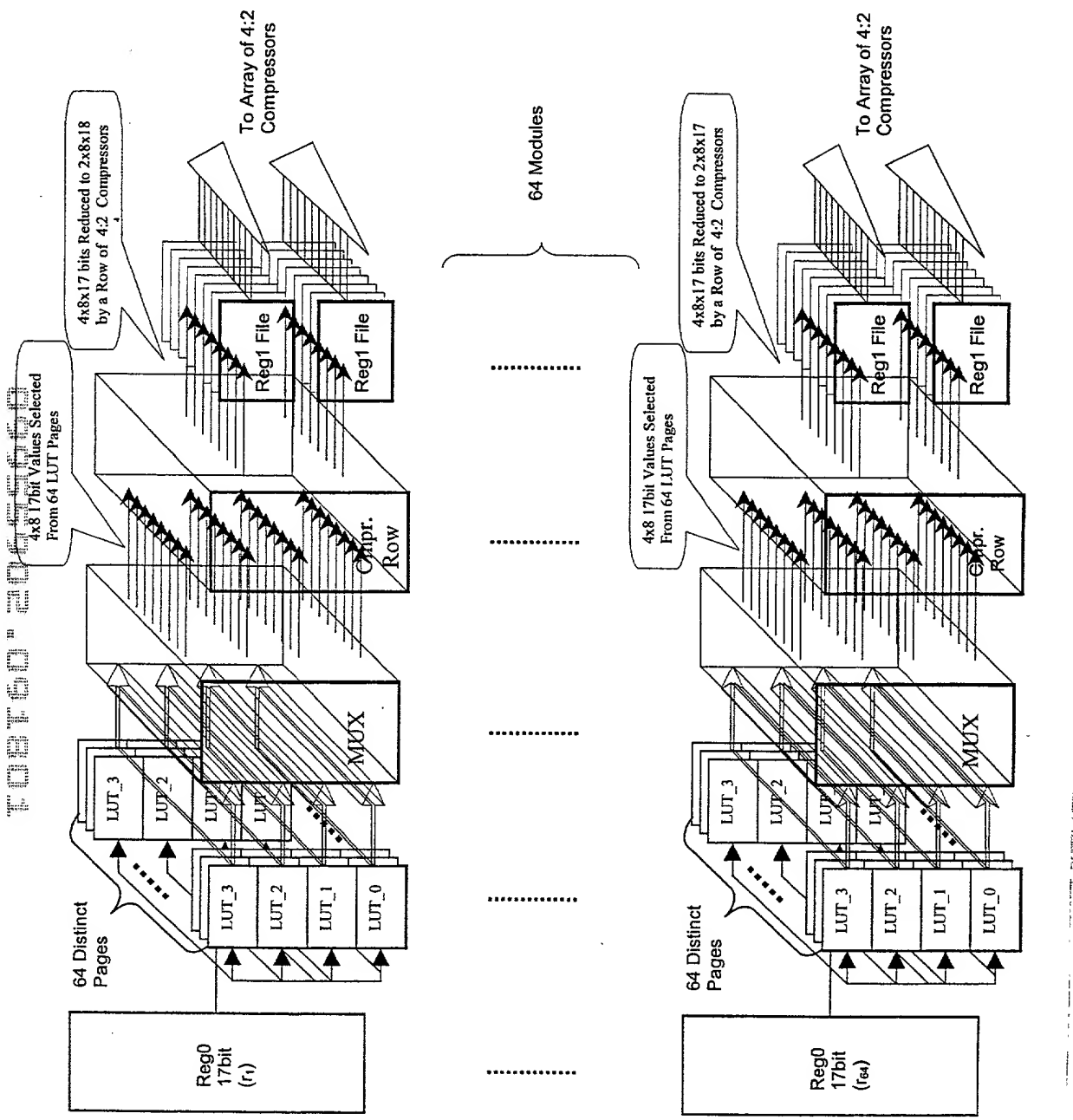

Reg0
17bit
(r_1)
64 Distinct
Pages
LUT_0
LUT_1
LUT_2
LUT_3
MUX
Compr.
Row
Reg1 File
Reg1 File
4x8x17 bits Reduced to 2x8x18
by a Row of 4:2 Compressors
To Array of 4:2
Compressors
4x8 17bit Values Selected
From 64 LUT Pages
64 Modules
Reg0
17bit
(r_{64})
64 Distinct
Pages
LUT_0
LUT_1
LUT_2
LUT_3
MUX
Compr.
Row
Reg1 File
Reg1 File
4x8x17 bits Reduced to 2x8x17
by a Row of 4:2 Compressors
To Array of 4:2
Compressors
4x8 17bit Values Selected
From 64 LUT Pages

FIG. 19

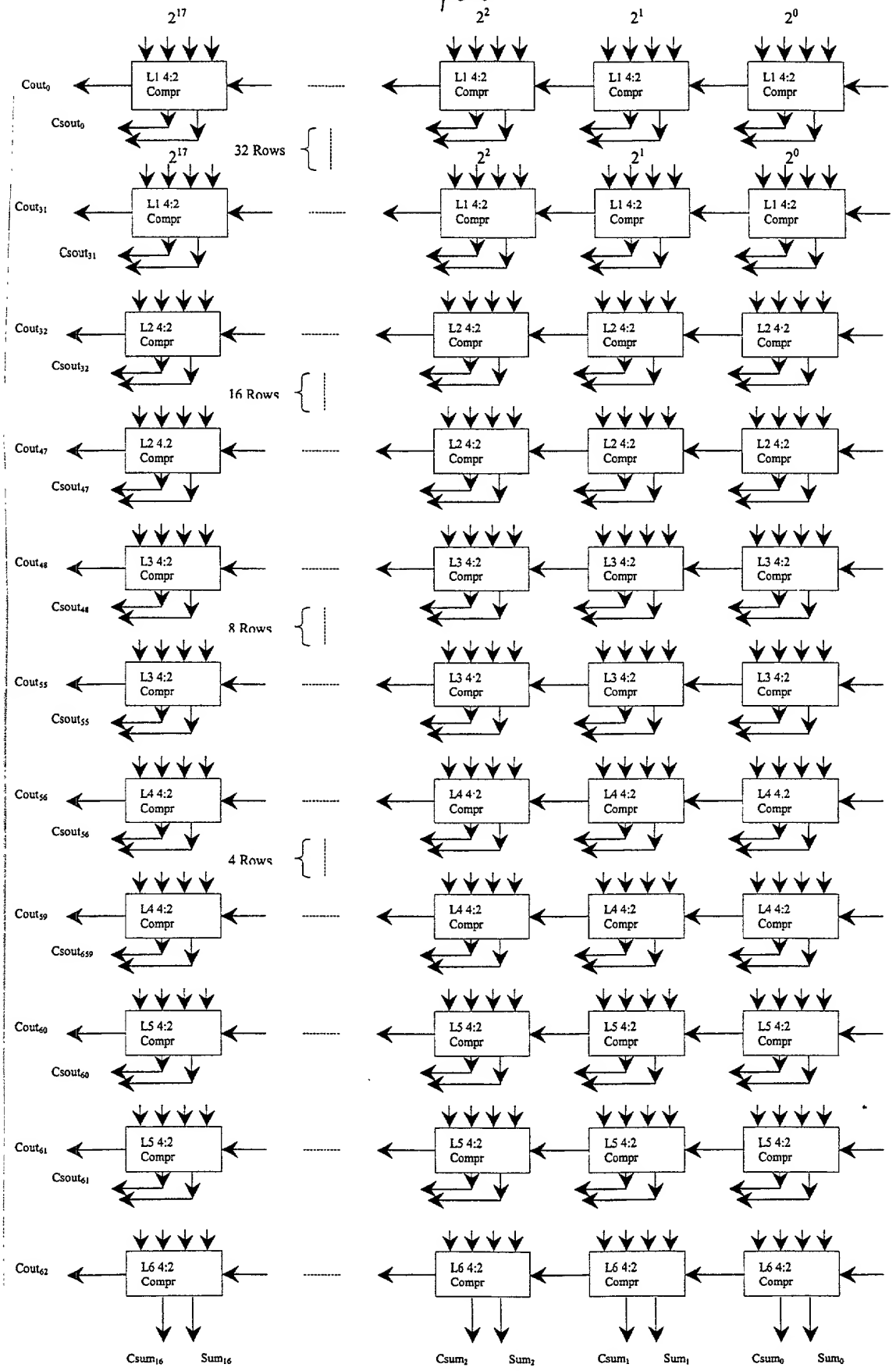


FIG. 20

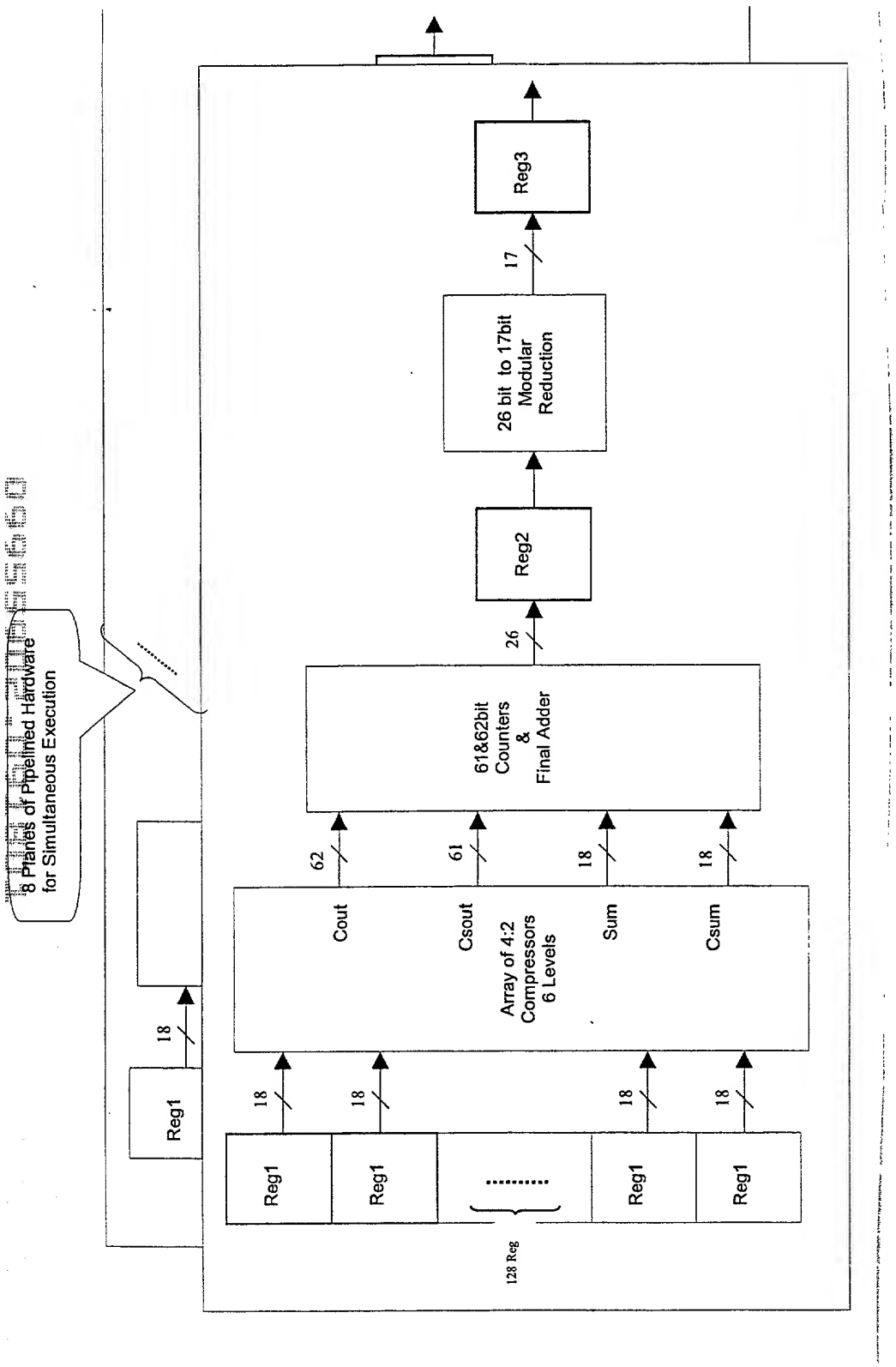

8 Planes of Pipelined Hardware for Simultaneous Execution
Reg1
18
Reg1
Reg1
Reg1
Reg1
Reg1
18
18
18
18
128 Reg
Array of 4:2 Compressors 6 Levels
Cout
Csout
Sum
Csum
62
61
18
18
61&62bit Counters & Final Adder
26
Reg2
26 bit to 17bit Modular Reduction
17
Reg3

FIG. 21

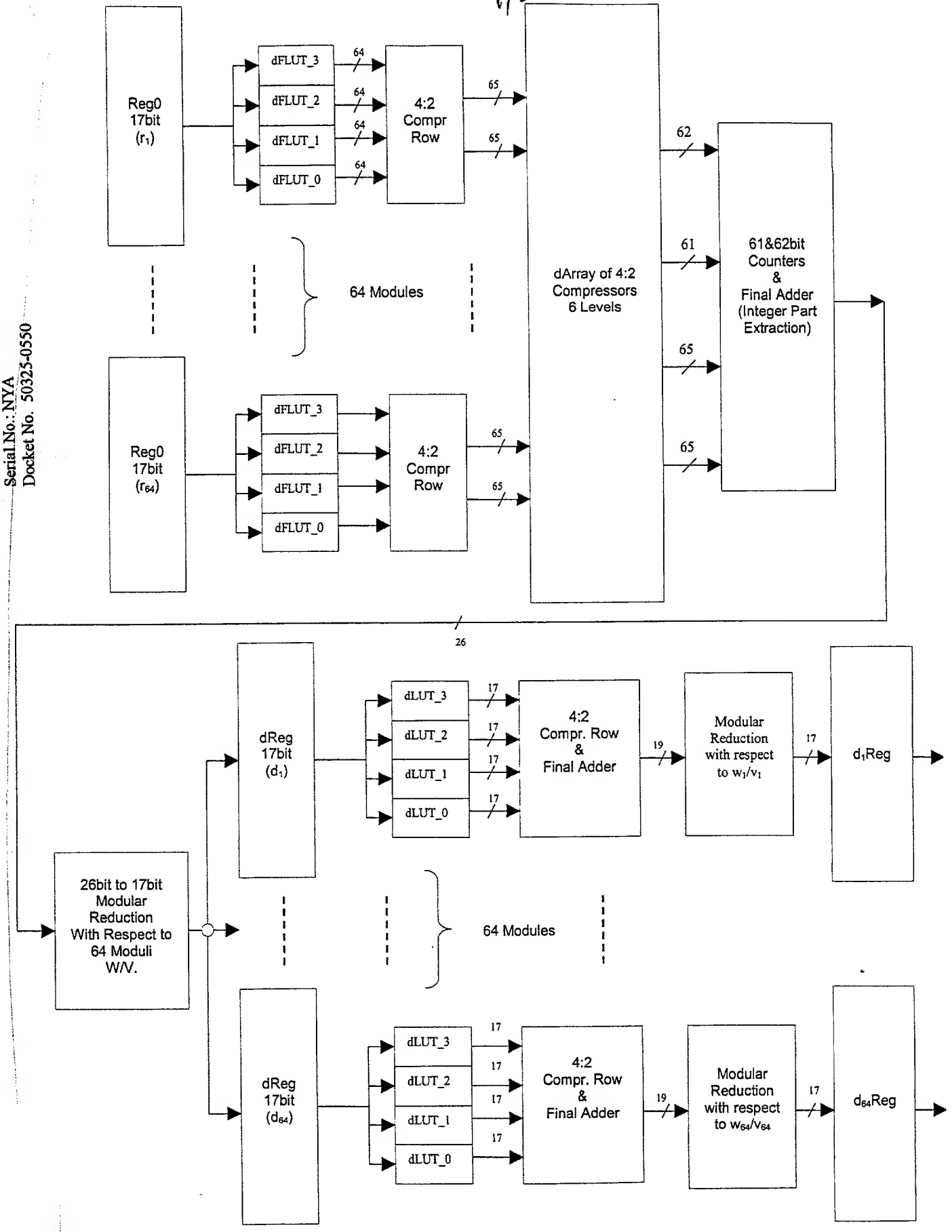
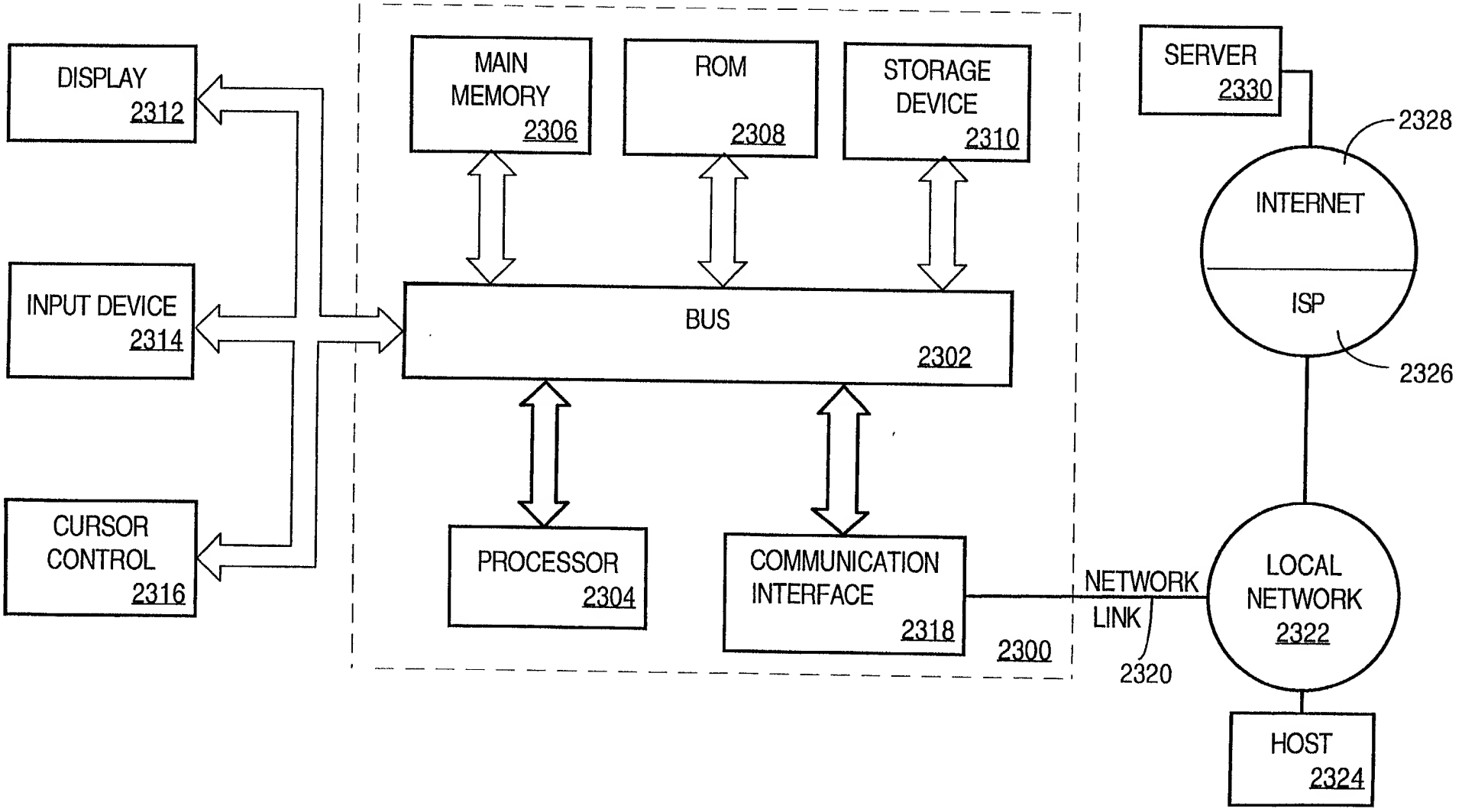


FIG. 22

FIG. 23


DISPLAY
2312
INPUT DEVICE
2314
CURSOR CONTROL
2316
MAIN MEMORY
2306
ROM
2308
STORAGE DEVICE
2310
BUS
2302
PROCESSOR
2304
COMMUNICATION INTERFACE
2318
2300
NETWORK LINK
2320
SERVER
2330
2328
INTERNET
ISP
2326
LOCAL NETWORK
2322
HOST
2324